National Infrastructure Protection Center
CyberNotes

Issue #2001-06 *March 26, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between March 4 and March 22, 2001. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alt-N [1]	Windows NT 2000	WorldClient 2.2.2	A Denial of Service vulnerability exists due to the way that requests for DOS devices are handled by the WorldClient and Webconfig service.	Upgrade available at: ftp://ftp1.deerfield.com/pub/current/wcsetup.exe	WorldClient DOS-Device Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Baltimore Technologies Inc. [2]	Windows NT 4.0	WEB sweeper 4.0	A Denial of Service vulnerability exists when a long HTTP request is sent through the Websweeper application.	The vendor suggests placing a firewall in front of the Websweeper application.	WEBsweeper Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Defcom Labs Advisory, def-2001-11, March 15, 2001.
[2] Defcom Labs Advisory, def-2001-10, March 8, 2001.

Vendor	**Operating System**	**Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/ Alerts**	**Common Name**	**Risk***	**Attacks/ Scripts**
Cisco[3]	Multiple	Aironet Firmware 8.07, 8.24, 7.0.x	A vulnerability exists in the web based interface which could allow a remote malicious user to view and alter the configuration of the bridge, even with the web-based management interface turned off.	Upgrade available at: ftp://ftp.cisco.com/pub/wireless/aironet	Cisco Aironet Web Administration Access	Medium	Bug discussed in newsgroups and websites.
Compaq Computer Corporation[4]	Windows 95/98/NT 4.0/2000, Unix	Insight Manager	A security vulnerability exists in the web-enabled software, which allows the software to act as a generic proxy server.	Update available at: http://www.compaq.com/support/files/server/us/index.html	Management Software Security Vulnerability	Low/**High** **(High for systems that are connected to multiple networks)**	Bug discussed in newsgroups and websites.
Debian[5] and Linux-Mandrake[6]	Unix	Ralf S. Engelschall ePerl 2.2.12, 2.2.13	A buffer overflow vulnerability exists due to several string operations being performed insecurely. If ePerl is installed 'setuid root,' which is an optional configuration, a malicious user may be able to execute arbitrary code with superuser privileges.	**Debian:** http://security.debian.org/dists/stable/updates/main/ **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	ePerl Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Denis Howe[7]	Windows NT 2000, Unix	Free Online Dictionary of Computing 1.0	A vulnerability exists because user supplied input isn't properly validated, which could let a remote malicious user compose and submit requests for files and execute certain commands with the privilege level of the webserver.	Vendor supplied patch: The main change is to check the filename from the QUERY_STRING: # Check for dodgy paths in file if ($file =~ m\|/\|) {print "Bad file \"$file\""; exit 0} and add a "<" to try to ensure that it is only opened for reading unless (open IN, "< $file") {print "Can't read $file: $!\n"; exit 0} Note: Patch will still allow reading of any file in the present directory.	Free Online Dictionary of Computing Remote File Viewing	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Elm Development Group[8]	Unix	Elm 2.5alpha3; HP-UX 11.0	A buffer overflow vulnerability exists in the '–s' (subject) argument which could let a malicious user gain elevated privileges, execute arbitrary code, and potentially read and alter other users' mail.	Upgrade available at: ftp://ftp.virginia.edu/pub/elm/elm2.5.3.tar.gz	Elm Subject Line Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[3] Cisco Security Advisory, CI-01.03, March 7, 2001.

[4] Compaq Computer Corporation/ Software Security Response Team, SSRT0715, March 22, 2001.

[5] Debian Security Advisory, DSA-034-1, March 7, 2001.

[6] Linux-Mandrake Security Update Advisory, MDKSA-2001:027, March 7, 2001.

[7] CGI Security Advisory #4, March 9, 2001.

[8] Securiteam, March 12, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
FreeBSD[9]	Unix	FreeBSD 3.x, 4.x; 3.5-STABLE & 4.2-STABLE prior to the correction date	A remote Denial of Service vulnerability exists when malformed packets are sent to the rwhod daemon.	To patch your present system: download the relevant patch from the below location, and execute the following commands as root: # fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-01:29/rwhod.patch # fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-01:29/rwhod.patch.asc	Rwhod Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Gordano[10]	Windows NT 4.0/2000	NTMail 6.0.3c	A Denial of Service vulnerability exists when a malicious user requests a malformed URL.	Patch located at: ftp://ftp.gordano.com/ntmail6/hotfixes/ntmail6C_Intel_20010317.zip	NTMail Web Services Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett-Packard[11]	Unix	HP-UX 10.0.1, 10.10, 10.20, 11.0	A Denial of Service vulnerability exists due to improper permissions on some of the files which could allow a malicious user gain elevated privileges.	Patches are available from Hewlett-Packard for HP-UX 10.01, 10.10, 10.20 and 11.00. For 10.10, 10.20 and 10.01, use PHSS_22935. For 11.00, use PHSS_22936. Patches located at: http://itrc.hp.com	HP-UX Series 700/800 asecure Denial of Service	Medium	Bug discussed in newsgroups and websites.
IBM[12]	Multiple	Net Commerce and WebSphere Commerce Suite 4.1 and previous	Several security vulnerabilities exist due to an unsecured macro vulnerability and an encrypted password vulnerability, which could let a malicious user execute arbitrary code. NOTE: A "hacker tool" has been published that could expose some web sites that have not taken preventive actions.	Implement the fixes located at: http://www-4.ibm.com/software/webservers/commerce/wcs_start/support.html	IBM Net. Commerce and WebSphere Encryption and Account Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit tool has been published. Vulnerability has appeared in the Press and other public media.
Ikonboard.com[13]	Windows NT 4.0/2000, Unix	Ikonboard 2.1.7b and previous	A vulnerability exists when a null byte is added to the name of a requested file which could let a remote malicious user read local files with the privileges of the web server. This would include sensitive system information, including account information and passwords for Ikonboard users and administrators.	No workaround or patch available at time of publishing.	Ikonboard Remote File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[9] FreeBSD Security Advisory, FreeBSD-SA-01:29, March 12, 2001.
[10] Defcom Labs Advisory def-2001-13, March 20, 2001.
[11] Hewlett-Packard Company Security Bulletin, HPSBUX0103-145, March 7, 2001.
[12] IBM Global Services, MSS-OAR-E01-2001:087.1, March 7, 2001.
[13] Securiteam, March 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Jelsoft Enterprises Ltd[14]	Multiple	vBulletin 1.0Lite, 1.1, 2.0beta 2	A vulnerability exists due to poor filtering procedures in the code that handles templates that could let a remote malicious user inject arbitrary code.	Commercial versions 1.1.6 and 2.0 beta 3 available at: http://www.jelsoft.com/index.html	vBulletin PHP Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
KICQ[15]	Unix	KICQ 1.	A vulnerability exists which involves received URLs that are passed to the web browser without any sanity checking which could allow a remote malicious user to execute arbitrary commands.	No workaround or patch available at time of publishing.	KICQ Remote Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
LICQ[16]	Unix	LICQ .85, 1.0.1, 1.0.2	A vulnerability exists which involves received URLs that are passed to the web browser without any sanity checking which could allow a remote malicious user to execute arbitrary commands.	No workaround or patch available at time of publishing.	LICQ Hostile URL Command Execution	**High**	Bug discussed in newsgroups and websites.
Matt Wright[17]	Unix	FormMail 1.0-1.6	A vulnerability exists in the FormMail.pl cgi-bin scripts which could allow a remote malicious user to send anonymous e-mail to arbitrary recipients.	No workaround or patch available at time of publishing.	FormMail Anonymous E-mail/ Spamming	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Michael Lamont[18]	Windows 95/98/NT 4.0/2000	Savant WebServer 3.0	A remote Denial of Service vulnerability exists when a specially crafted URL is requested.	No workaround or patch available at time of publishing.	Michael Lamont Savant Web Server Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[19] ***Security patch now available[20]***	**Windows 2000**	**Internet Information Services (IIS) 5.0**	**A Denial of Service vulnerability exists if WebDav is enabled and a specially crafted request is sent.**	***Frequently asked questions regarding this vulnerability and the patch can be found at:*** **http://www.microsoft.com/technet/security/bulletin/ms01-016.asp**	**IIS Malformed WebDav Request** **CVE name: CAN-2001-0151**	**Low**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Microsoft[21]	Windows 95, 98, ME, NT 4.0, 2000	Windows 95, 98, ME, NT 4.0, 2000	VeriSign, Inc., recently advised Microsoft that on January 29 and 30, 2001, it issued two VeriSign Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee. The common name assigned to both certificates is "Microsoft Corporation".	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-017.asp	Unauthenticated "Microsoft Corporation" Certificates	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press and other public media.

[14] Bugtraq, March 15, 2001.
[15] Securiteam, March 5, 2001.
[16] Securiteam, March 5, 2001.
[17] Bugtraq, March 10, 2001.
[18] Securiteam, March 12, 2001.
[19] Microsoft Security Bulletin, MS01-016, March 8, 2001.
[20] Microsoft Security Bulletin, MS01-016, revised March 13, 2001.
[21] Microsoft Security Bulletin MS01-017, March 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[22]	Unix	BeroFTPD 1.3.4; Proftpd 1.2.0; PureFTPd versions before 0.96	A Denial of Service vulnerability exists due to a file globbing bug, which can be exploited through a 'ls' command.	Contact your vendor for upgrade.	FTP Server Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[23, 24, 25] ***Debian releases patch***[26]	**Unix**	**Zope 2.3.1 b1 & prior**	**Multiple vulnerabilities exist: users can use through-the-web scripting capabilities to view and assign class attributes to ZClasses, possibly allowing them to make inappropriate changes; and there are security problems with the ObjectManager, PropertyManager, and PropertySheet classes.**	**RedHat:** **ftp://updates.redhat.com/powertools** **Linux-Mandrake:** **http://www.linux-mandrake.com/en/ftp.php3** **Conectiva Linux:** **ftp://atualizacoes.conectiva.com.br/** **FreeBSD:** **ftp://ftp.FreeBSD.org/pub/FreeBSD/ports** ***Debian:*** **http://security.debian.org/dists/stable/updates/main/source/zope_2.1.6-7.dsc**	**Multiple Zope Vulnerabilities**	**Medium**	**Bug discussed in newsgroups and websites.**
OReilly Software[27]	Windows 95/98/NT 4.0/2000	Website Professional 2.5.4	A vulnerability exists when a specially crafted URL is requested which could let a malicious user obtain the physical path to the root directory.	No workaround or patch available at time of publishing.	Website Professional Web Directory Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Palm[28] ***Vulnerability has appeared in the Press***[29]	**Multiple**	**Palm OS 3.3, 3.5.2**	**A vulnerability exists in the debugging mode which c ould let a malicious user with physical access to the PDA bypass the unit's password protections.**	**No workaround or patch available at time of publishing.**	**Palm Debugger Password Bypass**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Vulnerability has appeared in the Press and other public media.***

[22] List Digest, March 20, 2001.
[23] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:021-06, February 26, 2001.
[24] Linux-Mandrake Security Update Advisory, MDKSA-2001:025, February 26, 2001.
[25] Conectiva Linux Security Announcement, CLA-2001:382, March 2, 2001.
[26] Debian Security Advisory, DSA-043-1, March 9, 2001.
[27] Bugtraq, March 16, 2001.
[28] Securiteam, February 20, 2001.
[29] Network News, March 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Qualcomm[30]	Windows 95/98/NT 4.0/2000	Eudora 5.0.2	A vulnerability exists if the 'Use Microsoft viewer' option is enabled (even if the 'allow executables in HTML content' option is disabled), which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.eudora.com/cgi-bin/export.cgi?productid=EUDORA_win_510b12	Eudora 'Use Microsoft Viewer' Code Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
RediProducts[31]	Windows 95/98/ME/NT 4.0/2000	RediPlus 1.0	A vulnerability exists due to sensitive user information, including usernames and passwords, being stored on the client's system in cleartext in a log file used for troubleshooting. This file has a known default location, and could let a malicious user execute trades and carry out other financial activities.	Patch available at: http://www.redi.com/rpdownload.html	Redi Locally Readable Username/Password	**High**	Bug discussed in newsgroups and websites.
Rob Malda[32]	Unix	ASCDC 0.3	Multiple buffer overflow vulnerabilities exist which could let a malicious user gain root access and execute arbitrary code.	No workaround or patch available at time of publishing.	ASCDC Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Sentraweb[33]	Multiple	IndexU 1.0, 1.1, 2.0	A vulnerability exists by manipulating the cookies used by IndexU, which could let a remote malicious user gain admin privileges without a valid username or password.	Unofficial workaround (Undersec Security): Use .htaccess authentication to prevent users from accessing administrator area.	INDEXU Authentication Bypass	**High**	Bug discussed in newsgroups and websites.
SSH Communications Security Corp[34]	Windows	SSH Secure Shell for Windows Servers 2.4	A remote Denial of Service vulnerability exists due to adjacent connection handling.	No workaround or patch available at time of publishing.	SSH Secure Shell Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Microsystems[35]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the snmpXdmid mapper daemon, which could let a local or remote malicious user gain superuser access immediately.	No workaround or patch available at time of publishing.	Solaris snmpXdmid Buffer Overflow CVE name: CAN-2001-0236	**High**	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc.[36]	Unix	Solaris 8.0	A buffer overflow vulnerability exists in the SNMP Daemon, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Solaris SSP SNMPD Argument Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[30] Bugtraq, March 18, 2001.
[31] Bugtraq, March 20, 2001.
[32] Wkit Security Advisory, WSIR-01/02-06, March 8, 2001.
[33] Undersec Security Advisory, March 4, 2001.
[34] USSR Labs, USSR-2001001, March 15, 2001.
[35] Bugtraq, March 14, 2001.
[36] Securiteam, March 14, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SWSoft[37]	Windows NT 4.0/2000, Unix	ASPSeek 1.0, 1.0.1, 1.0.3	Several buffer overflow vulnerabilities exist in the s.cgi script, which could let a remote malicious user execute arbitrary code.	Patch available at: http://www.aspseek.org	ASPSeek s.cgi Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
TYPSoft[38]	Windows 95/98/ME/ NT 4.0/2000	TYPSoft FTP Server 0.85	A directory traversal vulnerability exists in the FTP GET command, which could allow a remote malicious user to obtain files outside the permitted directory.	Upgrade available at: http://www.multimania.com/typsoft/eng/	TYPSoft FTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Valve Software[39]	Windows 95/98/ME/ NT 4.0/2000, Unix	Half-Life 1.1.0.4 Linux; 1.1.0.4 Windows	Several vulnerabilities exist: two buffer overflow vulnerabilities and a string formatting vulnerability, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: ftp://ftp.sierra.com/pub/patches/pc/hl1106.exe	Half-Life Buffer Overflow Vulnerabilities and String Formatting Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Veritas Software[40]	Unix	Cluster Server 1.3solaris	A Denial of Service vulnerability exists in the '-L' command option.	Patch available at: ftp://ftp.veritas.com/pub/support/i57214.lltstat-fix.tar.Z	Cluster Server -L Denial of Service	Low	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system and/or the intruder can execute or alter arbitrary system files. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between March 8 and March 20, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 22 scripts, programs, and net-news messages containing holes or exploits were identified. NOTE: At times, scripts/techniques may contain names or content that may be considered offensive.

[37] Securiteam, March 21, 2001.
[38] Securiteam, March 6, 2001.
[39] Securiteam, March 12, 2001.
[40] eSecurityOnline Free Vulnerability Alert 3436, March 5, 2001.

Date of Script (Reverse Chronological Order)	Script name	Script Description
March 20, 2001	Ettercap-0.3.0.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
March 20, 2001	**Stick.tgz**	**An attack tool that targets IDS systems.**
March 19, 2001	**Formatstring.pdf**	**Document titled "Exploiting Format String Vulnerabilities".**
March 19, 2001	Ftpsed.pl	Perl script which exploits a Denial of Service vulnerability in Proftpd v1.2 and below.
March 19, 2001	VV5.pl	A remote Denial of Service exploit for the IIS 5.0 / Windows 2000 WebDav vulnerability.
March 16, 2001	Joe28.c	Script which exploits the Joe 2.8 vulnerability.
March 15, 2001	Ascdcx.c	Local exploit for the /usr/X11R6/bin/ascdc v0.3-2-i386 vulnerability.
March 15, 2001	Hjksuite-0.1b.tar.gz	A collection of programs for hijacking that contains hjklib, a library for hijacking. It also contains programs like hjkbnc that allows IRC hijacking directly with your client, hjkhttpd for hijacking HTTP sessions, and hjknetcat, for hijacking text connections.
March 15, 2001	Mdcrack-0.6.tar.gz	A brute forcer for MD5 hashes, which is capable of breaking up to 6 character passwords within hours, and 8 character passwords within two days.
March 15, 2001	Nmap-2.54BETA22.tgz	A utility for port scanning large networks.
March 15, 2001	Openssh-2.2.0-exp.tgz	Remote exploit for the OpenSSH-2.2.0 vulnerability.
March 15, 2001	Rnmap_0.5-beta.tar.gz	A remote python client/server package which allows many authorized clients to connect to a centralized nmap server to do port scanning.
March 15, 2001	Spc001.zip	Share Password Checker acquires the list of shared folders of a Windows 95/98/Me machine on the network and shows you those folders' passwords. This tool acquires the list of the shared folders also for Windows NT/2000 machines, but it only distinguishes folders which have no password. "Share Password Checker" exploits the "Share Level Password" Vulnerability.
March 15, 2001	Sqlping.c	A tool which sends a specially crafted UDP packet to port 1434 to SQL Server 2000 which will return useful information including SQL version and service pack.
March 15, 2001	Suq_diq.zip	A remote exploit for IBM Net.Commerce, WebSphere, and possibly other IBM and Lotus applications, which reveals the usernames and plaintext passwords of Net.Commerce accounts. Also includes exploit URL's.
March 15, 2001	Winfingerprint.zip	Advanced remote Windows OS detection.
March 13, 2001	Diablomin.zip	An advanced keystroke logger for Windows that features the ability to send logs to an FTP account, make .exe server side files, e-mail notification, encryption and compression, and more.
March 13, 2001	Getacct001.zip	Tool which lets a malicious user retrieve sensitive information about users and accounts.
March 9, 2001	Cgiproxy.1.4.1-SSL.tar.gz	A Perl CGI script that acts as an Internet proxy that can retrieve resources that may be inaccessible from your own machine.
March 9, 2001	Ettercap-0.2.4.tar.gz	A network sniffer/interceptor/logger for switched LANs, which uses ARP poisoning and the man-in-the-middle technique, to sniff all the connections between two hosts.

Date of Script (Reverse Chronological Order)	Script name	Script Description
March 9, 2001	Scanssh-1.5.tar.gz	Scans a list of addresses running networks for SSH and their version numbers. Also supports random selection of IP addresses from large network ranges and is useful for gathering statistics on the deployment of SSH servers in a company or the Internet.
March 8, 2001	**ascdc-ex.c**	**Script which exploits the ASCDC Buffer Overflow vulnerability.**

Trends

Probes/Scans:

There has been an increase in the number of suspicious probes and scans designed to find vulnerable domain name servers on corporate networks.

Backdoor-G and NetBus Trojan scans have increased in number.

Other:

A new worm, Linux.Lion.Worm, appears to be spreading rapidly across the Internet. It scans the Internet looking for Linux computers with the BIND TSIG vulnerability. It infects the vulnerable machines, steals the password file (sending it to a China.com site), installs other hacking tools, and forces the newly infected machine to begin scanning the Internet looking for other victims. For more information, please see the Virus Section and NIPC ADVISORY 01-005, located at http://www.nipc.gov/warnings/advisories/2001/01-005.htm.

A new version of a Trojan horse program, SubSeven 2.2, that is popular with computer intruders has been publicly released on the Web. For more information, please see Trojan Section.

On January 29 and 30, 2001, VeriSign, Inc. issued two certificates to an individual fraudulently claiming to be an employee of Microsoft Corporation. Any code signed by these certificates will appear to be legitimately signed by Microsoft when, in fact, it is not. For more information, please see NIPC ADVISORY 01-006, located at: http://www.nipc.gov/warnings/advisories/2001/01-006.htm, or CERT® Advisory CA-2001-04, located at: http://www.cert.org/advisories/CA-2001-04.html.

A software package has been released which, if used maliciously, may disable a victim's computer or network's IDS by flooding it with Internet traffic emanating from several random Internet Protocol (IP) addresses simultaneously. For more information, please see NIPC ASSESSMENT 01-004, located at: http://www.nipc.gov/warnings/assessments/2001/01-004.htm.

A new technique has emerged that exploits vulnerabilities in Windows machines installed with IIS 4.0 or 5.0. A Windows NT/2000 utility called "FireDaemon" is being used as a part of a toolkit to further compromise the machines. For more information, please see the security advisory located at: http://www.firedaemon.com under the "Security Alert" posted on March 7, 2001.

Recent attacks against e-commerce and e-banking sites are being carried out via known vulnerabilities for which patches have been available for months or, in some cases, years. For more information, please see NIPC Advisory 01-003, located at: http://www.nipc.gov/warnings/advisories/2001/01-003.htm.

A script that exploits the BIND INFOLEAK and TSIG vulnerability has been released. Users are advised to update their BIND server if they haven't already done so.

The CERT/CC has recently learned of four vulnerabilities spanning multiple versions of the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) server. Because the majority of name servers in operation today run BIND, these vulnerabilities present a serious threat to the Internet infrastructure. For more information, please see CERT® Advisory CA-2001-02, located at: http://www.cert.org/advisories/CA-2001-02.html.

Viruses

A list of viruses infecting two or more sites as reported to various anti-virus vendors and virus incident reporting organizations has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table list the viruses by: ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. These types of malicious code will also now be included in the table. Following this table are write-ups of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **225** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **652** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Hybris	Worm	Stable	November 2000
2	VBS/Kakworm	Script	Slight increase	December 1999
3	PE_MTX.A	File Infector, Trojan	Slight decrease	September 2000
4	W32/Navidad	File, Worm	Stable	November 2000
5	VBS/LoveLetter	Script	Stable	March 2000
6	VBS/SST	Script, Worm	Stable	February 2001
7	W32/FunLove	File	Return to table	November 1999
8	W32/SKA	File	Slight decrease	March 1999
9	W32/Prolin	Worm	Return to table	December 2000
10	W97M Ethan.A	Macro	Return to table	February 1999

Linux.Lion.Worm (Linux Worm): This is a dangerous Linux worm that infects computers running Linux. This worm is similar to Linux.Ramen and does not execute on systems running Microsoft Windows. It appears to spread using a known BIND TSIG vulnerability discovered early in 2001 to spread. The worm will create multiple backdoors on the system by replacing some critical files. The worm also exports password and other critical information to the hacker, which allows them to utilize the backdoors.
The Lion worm spreads via an application called "randb". Randb scans random class B networks probing TCP port 53. Once it hits a system, it checks to see if it is vulnerable. If so, Lion exploits the system using an exploit called "name". It then installs the t0rn rootkit. Once Lion has compromised a system, it:

- Sends the contents of /etc/passwd, /etc/shadow, as well as some network settings, to an address in the china.com domain.
- Deletes /etc/hosts.deny, eliminating the host-based perimeter protection afforded by TCP wrappers.
- Installs backdoor root shells on ports 60008/tcp and 33567/tcp (via inetd, see /etc/inetd.conf)
- Installs a trojaned version of ssh that listens on 33568/tcp
- Kills Syslogd, so the logging on the system can't be trusted
- Installs a trojaned version of login

- Looks for a hashed password in /etc/ttyhash /usr/sbin/nscd (the optional Name Service Caching daemon) is overwritten with a trojaned version of ssh.

The t0rn rootkit replaces several binaries on the system in order to conceal itself. It replaces the following binaries: du, find, ifconfig, in.telnetd, in.fingerd, login, ls, mjy, netstat, ps, pstree, and top.

OXP/Listi.A (Aliases: W97M/Listi.A, XP.Kallisti) (OfficeXP Macro Virus): This is the first macro virus coded for OfficeXP Word. The virus does not have a damaging payload; however it may play an audio message if Microsoft Agent is installed and the audio system hardware is configured and available for use within OfficeXP.

PE_ILMX.A (Aliases: ILMX, W95/ILMX, Win95.ILMX, W95.ILMX.1291) (Win 32 Virus): This is a polymorphic, memory-resident Win32 virus that executes in Windows 95/98 operating systems. The virus uses XOR encryption with a variable key to achieve simple polymorphism. Its decryption routine is patched from Entry Point. It encrypts and stores infected files in its virus body. Once it is active in memory, it infects all files that are accessed thereafter. It does not contain a destructive payload and does not drop or modify any file or registry entry. This virus uses the Service Interrupt Descriptor Table by hooking Interrupt 3 to achieve Ring Zero privileges. Once it is in Ring Zero, it hooks the IFS Manager and then waits for the IFSFN_Open function to be invoked, which happens when a file is accessed. If a file contains an .EXE or an .SCR extension and is not infected, it attaches itself to the file. It identifies infected files with the FMX marker so that it does not reinfect a system.

PHP_CARACULA.A (Alias: CARACULA.A) (PHP Script Worm): This worm propagates via Internet Relay Chat (mIRC). It appends itself at the end of HTM, HTML, and PHP files and also overwrites files in the Windows System directory that end with .EXE, .OCX, .SYS, .BAT, and .VXD.

VBS/Angel@MM (Alias: VBS.Rewind.A@mm (NAV)) (Visual Basic Script Worm): This VBScript worm attempts to mail itself to all recipients in the Microsoft Outlook address book and drops the W95/CIH.1122 file infector virus. When run, the script copies itself to the WINDOWS TEMP directory as T4UMHF5.vbs and drops the file ALE32.EXE (detected as W95/CIH.1122) in the same directory. It then attempts to mail itself to all recipients found in the Microsoft Outlook address book. It creates a registry run key value to load the script at startup:

HKLM\Software\Microsoft\Windows\CurrentVersion\
RunServices\T4UMHF5=C:\WINDOWS\TEMP\T4UMHF5.VBS

Before exiting, the script executes the ALE32.EXE file, in turn loading W95/CIH.1122 into memory. The script contains the text AlevirusSCS VxBrasil :) while the .EXE contains the text AlevirusSCS v666 VxBrasil.

VBS/Linda-A (Visual Basic Script Worm): This is a Visual Basic Script worm, which spreads via e-mail, IRC (Internet Relay Chat) and across networks. When it is run, it will create a copy of itself named XMLDriver32.dll.vbs in the Windows system directory. The worm searches on local and network drives for files with any of the following extensions: VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA, JPG, JPEG, MP3, MP2, XML, PHP3, HTM, WAV, BMP, DOC, RTF, XLS, PPT, WRI, MDB, ZIP, RAR, ARJ, PDF, MID, GIF, AVI, HLP, FRM, MP4, C, PL, PAS, PS, TIF, WPD, FM, MK5, ASP, TXT, CHM, GZ, TAR, WSC, MHT, HTT, LHA, LZH, PCX, or PIF. If the worm finds a suitable file, it will create a copy of itself, using the same name and adding .VBS to the end. It will then delete the original file. If the worm determines that the mIRC Internet Relay Chat client is installed, it will also create a file named 'script.ini' in order to send copies of the virus to other IRC users. It will then use Microsoft Outlook to send e-mail to addresses found in the user's address book. The e-mail it sends has the following characteristics:

Subject: Important message for <recipient name>
Body text: This is the attached file you asked from me.

The attached infected file may have any name.

VBS/LoveLet-CG (Visual Basic Script Worm): This virus is a variant of the VBS/LoveLet-G e-mail aware worm. You will typically receive the worm in the form of an e-mail attachment called IMPORTANT-COMPANY-NEWS.HTM.vbs. If executed the worm will drop three files into the root directory of the drive:

\MSKernel32.vbs
\Win32DLL.vbs
\IMPORTANT-COMPANY-NEWS.HTM.vbs

The worm forwards itself as an e-mail attachment to all addresses in the Outlook address book. The worm contains the following remarks inside its code but does not display them:

```
Rem Iraqi-freeiraq(vbe) <The US/UK Government SUCKS>
Rem by: Morpheus / youvebeentangod@mail.com /
    @BRITVIC Soft / Bagdad, IrAQ
Rem You Know when you've been tango'd
```

VBS/Postcard@MM (Aliases: Postcard worm (CA), VBS.Postcard@MM (NAV)) (Visual Basic Script Worm): This virus creates files which do not display a visible extension in Windows, even if Windows is configured to show all files and to display extensions. It uses an exploitable method of using CSLID values for extensions of files created. By doing this, the extensions are hidden and not visible. This is a function of Windows itself. This is a polymorphic VBScript worm that mails itself to all Microsoft Outlook address book recipients. It infects .ASP, .HTM, .HTML, and .SHTML files in the Windows, Windows\System, and Windows\Temp directories by adding its infectious script code to the end of these files. In addition, the script attempts to copy itself to the root level of mapped drives.

VBS/Staple-A (Aliases: VBS/Injustice-A, VBS/Staple.A@mm) (Visual Basic Script Worm): This is a Visual Basic Script worm which uses Microsoft Outlook to replicate. The worm arrives in an e-mail message with the following characteristics:

Subject:
RE:Injustice
Message body:
Dear <name>
Did you send the attached message. I was not expecting this from you !
Attached filename: injustice.txt.vbs

If the attached file is executed, it counts the number of addresses in the Outlook address book and sets a variable to either 50 or to the number of address book entries if the number is less then 50. It then uses Outlook to send the worm file to randomly chosen entries from Outlook's address book. It sends this e-mail only once for every chosen address. The worm then runs Internet Explorer and opens the following URLs, each in a new window:

www.sabra-shatila.org
www.petitononline.com/palpet/petition.html
www.palestine-info.org
freesaj.org.uk
hanthala.virtualave.net
www.ummah.net/unity/palestine/index.htm

The websites appear to be pro-Palestinian political websites.

W32/Magistr-A (W32 Executable File Virus): This virus is polymorphic and spreads using both e-mail and file infection techniques. It also carries a destructive payload containing code similar to the hardware destroying Kriz virus. Like Kriz, Magistr can destructively flash a PC's BIOS as well as overwrite data. If users click on the executable attachment of an infected message they risk have their data overwritten and replaced by text files containing the message: "You think you are God, but you are only a piece of shit". The virus searches a user's address book, mailboxes and other files present on an infected machine for e-mail addresses. It specifically targets addresses from Outlook Express, Netscape Navigator and Internet Mail and News. Once a list of e-mail addresses has been obtained, Magistr sends itself to these addresses along with five other Word or text files using its own e-mail client.

W32/Scrambler.g@MM (Aliases: I-Worm.Xanax, Win32.HLLP.Xanax, Xanax.exe) (Win32 Virus): This is a prepending virus for Windows. This virus will also attempt to distribute itself via Outlook, and also through mIRC. This virus may arrive to users connecting to mIRC as a file named xanax.exe. The following string exists in the virus dropper XANAX.EXE; however, it is not displayed:

Win32.HLLP.Xanax (c) 2001 Gigabyte

W97M.Goober.E (Word 97 Macro Virus): This is a stealth macro virus that infects the active document and the Normal.dot template. Certain words in the active document may be replaced. The virus t urns off the options that may alert you to its presence. When a new document is created, W97M.Goober.E saves its source code in the C:\G00ber.sys file and then inserts that viral code in both the Normal.dot template and the active document. When opening a document, W97M.Goober.E also does the following:

Replaces all instances of "ShiThe!" with "The"
Replaces all instances of "shithe!" with "the"

W97M.Marker.EN (Word 97 Macro Virus): This is a variant of W97M.Marker. It always infects the Normal.dot template. It can also infect the active document. The virus has a date-triggered payload. If the year is 2000 or later and the month is July or later, the virus will create 999,999,991 copies of the active document in the \Windows folder.

WM97/Bablas-BK (Word 97 Macro Virus): This is a variant of the WM97/Bablas Word macro virus. The virus changes the application status bar and caption to display messages in non-English characters when infecting the system. The virus displays similar messages if the user tries to access the Help|About menu option, and if an infected file is opened on a Friday or Sunday before 9:00 p.m.

WM97/Ded-M (Word 97 Macro Virus): WM97/Ded-M is a Word macro virus, which infects Microsoft Word documents. The virus has been created by an interaction between two other Word macro viruses: WM97/Ded-B and WM97/Class.

M97/Ded-N (Word 97 Macro Virus): This is a variant of the WM97/Ded-B macro virus. Unlike other family members, this variant has no polymorphic capabilities and no malicious payload.

WM97/Doccopy-A (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents. The virus creates an infected file called saver.dll in the directory that Microsoft Word has been run from. The virus also creates a subdirectory under Microsoft's Word directory called Doc_Copy into which it places copies of infected files.

WM97/Flop-A (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents. If you open a Word document from a floppy disk on an infected system, the virus will copy the file from the floppy disk into the TEMP directory on the hard drive. The file is given a random .TMP filename plus hidden, system and read-only attributes. The virus will infect both this file and the file on the floppy disk.

WM97/Marker-GN (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents. The virus changes the file summary information to:

Author: "M.E".
Comments: "Accept no Bullshit!"

WM97/Myna-AK (Word 97 Macro Virus): This is a variant of the WM97/Myna-D Word macro.

WM97/Myna-AL (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents. Like earlier family members, the WM97/Myna-AL virus contains no intentionally malicious payload other than replication. The virus contains the phrase MYNAMEISVIRUS, which is used as a flag to check to see whether it has already infected a file. WM97/Myna-AL has also interacted with a member of the WM97/Marker virus family so that whenever a document is closed there is a 1 in 3 chance of a File Summary box appearing on the screen with the author's name set to Ethan Frome.

WM97/Opey-X (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents. If the month if later than July, the virus makes the following alterations to the document's user details:

User name = "Crazy Man"
User address = "LBTMM B'99 PHILIPPINES"
User initials = "Crazy"

The virus will also alter the file summary information to:

Author = "Crazy Man"
Title = "Crazy"
Manager = "MMA"
Company = "Crazy Man Company"
Comments = "HELLO I am the Crazy Man From the Crazy World of
Computer. Don't you worry I'm not as crazy than you think...".

If the user tries to access the Tools/Macro menu, the virus will display a message box containing the phrase "AHA! You want to know about my Macro Code.. Kill Me FIRST..." At 3:00 p.m., it displays another message box containing the text "It's 3:00 P.M., Please Pray The salvation of your Life, cause you don't know it's is the time for you to die..." before exiting Microsoft Word. If the time is 12:05 p.m., the virus displays another message; "It's 12:00 it's time for Lunch…" before exiting Microsoft Word.

WM97/Pizdec-A (Word 97 Macro Virus): WM97/Pizdec-A has a main function named Virus that is called when you open or close a document. In addition, a message box containing non-English characters will appear when you choose any of the following options from the menu bar:

Help|About
File|Save
File|SaveAs
File|Print
File|PageSetup
Tools|Macro
File|Templates

The same message appears if you attempt to view the VB virus code. The virus also contains a function Pizdec, which will display another message box containing non-English characters seven days after the first infection.

WM97/Wrench-H (Word 97 Macro Virus): This is a minor variant of the WM97/Wrench family of macro viruses. The virus drops a file called "ascii.vxd" in the root directory. This file contains a listing of the virus code. It has no malicious payload.

XM97/Divi-AE (Excel 97 Macro Virus): This is a variant of the XM97/Divi-A Excel macro virus. It creates a file called BASE5874.XLS in the Excel template directory, and will infect other spreadsheets when they are opened or closed. The virus adds a flag, in the form of a variable called IVID plus a hexadecimal number, to each file as it is infected. The virus uses this flag to determine whether the spreadsheet has already been infected.

XM97/Squared-A (Alias: X97M.Self.A) (Excel 97 Macro Virus): This virus creates the file "nt².xls" (nt<squared>.xls) in the XLSTART directory. It has no malicious payload.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	**N/A**	**Current Issue**
Backdoor.Quimera	**N/A**	**Current Issue**
Backdoor-JZ	N/A	CyberNotes-2001-02
BAT.Install.Trojan	N/A	CyberNotes-2001-04
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
Flor	N/A	CyberNotes-2001-02
HardLock.618	N/A	CyberNotes-2001-04
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAINABEL151	**1.51**	**Current Issue**
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_Q2001	**N/A**	**Current Issue**
TROJ_QZAP.1026	N/A	CyberNotes-2001-01

Trojan	Version	CyberNotes Issue #
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	**.22**	**Current Issue**
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	**2.2**	**Current Issue**
TROJ_SUB722_SIN	**N/A**	**Current Issue**
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.RASDialer	**N/A**	**Current Issue**
Trojan.Sheehy	N/A	CyberNotes-2001-05
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
W32.BatmanTroj	N/A	CyberNotes-2001-04

Backdoor.NTHack: This is a backdoor Trojan that steals passwords and does the following:

1. It first executes the DL.bat file. When DL.bat is executed, this batch file changes the current folder to \Inetpub\scripts and attempts to connect to a specific Web site using TFTP. Once connected, it attempts to download the DL.exe file.
2. The batch file then checks to see if DL.exe has been downloaded. If it has, it starts this executable.
3. DL.exe is a Visual Basic program packed with UPX. Upon execution, this program attempts to connect to the IP address 216.205.125.115 using FTP and download 14 files named 00.d, 01.d, and 02.d through 13.d.
4. Once the files have been downloaded, DL.bat renames 00.D to Install.bat. It then removes the read-only attribute on the TFTP program and on DL.exe, and attempts to delete these two files. Install.bat is then called for execution.
5. When Install.bat is executed, it renames the other 13 files to the following:
   01.d -> Dir.txt
   02.d -> FireDaemon.exe
   03.d -> Login.txt
   04.d -> MMtask.exe
   05.d -> NewGina.dll
   06.d -> Reggina.exe
   07.d -> Regit.exe
   08.d -> Restrict.exe
   09.d -> Restsec.exe
   10.d -> Settings.reg
   11.d -> SUD.exe
   12.d -> Makeini.exe
   13.d -> SUD.ini
6. Most of these programs are legitimate programs (such as a packed version of Regedit.exe), but the backdoor Trojan utilizes these for malicious purposes. These files are deleted after the Trojan is finished using them.
7. A temporary file that is used as a log file for the administrator's passwords may also be created. Changed passwords are also captured in this file.

Backdoor.Quimera: Backdoor.Quimera is a Trojan horse that allows unauthorized access to your computer. Backdoor.Quimera is sent as an executable installation package. The executable file displays a Setup icon. When the file is run, it does the following:

1. It inserts the following files on the system:
   C:\~setup.t\Mswinsck.ocx
   C:\~setup.t\Teste.exe
   C:\~setup.t\Vb40032.dll
2. After these files are extracted by the installer, Teste.exe is run. Teste.exe is a Visual Basic compiled executable that needs Vb40032.dll to run. The Mswinsck.ocx file is used to establish a connection over the Internet.
3. Teste.exe then registers the Mswinsck.ocx to the system, so that it is used when working with sockets.
4. Next, it adds the value modem1C:\WINDOWS\NETCOM1.EXE to the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. This causes Netcom1.exe to be executed when Windows starts.
5. Teste.exe then inserts a copy of itself as C:\Windows\Netcom1.exe, so that the added registry key can be executed.
6. Finally, it copies Vb40032.dll and Mswinsck.ocx from C:\~setup.t to C:\Windows\System.

TROJ_CAINABEL151 (Aliases: Cain v1.51, CAINABEL 151, Abel v1.1): This is a password recovery and password management application for Windows 9x systems that is owned by Break-Dance (www.confine.com) and is distributed as freeware. It contains limited remote access capability and enables a remote user to retrieve and change the passwords of an infected system.

TROJ_Q2001 (Aliases: TROJ_Q2001.C, TROJ_Q2001.S, Q2001): This Backdoor Trojan is similar to the BACK ORIFICE and SUBSEVEN Trojans that allow remote control over an infected computer. It consists of a Server and a Client component. The Server component is the program used on a target system and the CLIENT component is the controlling program. The Client side of this Trojan asks for the IP address of the infected machine that is running its Server component, to which it connects itself. It cannot establish a connection to an infected computer when the server side is not running. The server side of this Trojan is the program loaded on the host computer. Upon execution, it registers itself in the system so that it automatically runs at every Windows Startup. When a connection is established between the Server and Client components, the user of the Client side can remotely access the infected system.

Trojan.RASDialer: This is a malicious Trojan horse that attempts to connect to a BBS service. This could result in excessive charges on your phone bill. When Trojan.RASDialer is executed, it uses Remote Access Service (RAS) to dial out. After it connects to a BBS service, it runs your default Web browser. (The Trojan looks at the Windows registry to see which browser is used by default to open HTML files.) It then tries to connect to the URL http:/ /69.69.69.69.

TROJ_SUB722 (Aliases: SubSeven 2.2, BackDoor-G22, Backdoor.SubSeven.22.a, TROJ_SUB722_P1, TROJ_SUB722_P2, TROJ_SUB722_P3, TROJ_SUB722_P4, TROJ_SUB722_P5, TROJ_SUB722_P6, TROJ_SUB722_P7, TROJ_SUB722_P8, TROJ_SUB722_P9, TROJ_SUB722_P10): This Trojan is a new member of the SubSeven family of backdoor programs. This new variant has several enhancements and new functionality compared to its predecessors. This Trojan, like other backdoor Trojans, has a client and server component. A remote user running the client component of this Trojan can get full access to a system infected with the server component of the Trojan. This Trojan compromises network security because the server side gives the client side full administrative privileges. Both the server side and the client side are customizable, and new functions can be introduced into them, as they support plug-ins. In addition, this variant also has a component called EditServer. The EditServer program allows the remote user to create a customized version of the server, permitting the client side to configure the functionality and behavior of the server. The remote user running the client side gets full control of the infected system and is allowed to perform several functions depending upon the plug-in that has been installed. The plug-ins for this Trojan and their functionality are:

TROJ_SUB722_P1: Steals ICQ Password by displaying a fake ICQ password screen
TROJ_SUB722_P2: Matrix effect when sending message to victim
TROJ_SUB722_P3: Packet sniffer
TROJ_SUB722_P4: App redirect, Netstat, Port redirect, FTP server, Process manager (view/kill running task/applications), Registry editor (allows you Create/delete registry entries) and Network browser
TROJ_SUB722_P5: Take screenshots, track mouse movements and view webcam
TROJ_SUB722_P6: Flip screen, Display picture, Edit clipboard, Print text, Text2speech and Play tic-tac-toe
TROJ_SUB722_P7: Open Web browser, Change resolution, Change windows colors, Restart computer, Change sound settings, Change time/date settings and Play with keyboard lights
TROJ_SUB722_P8: Keylogger, Disable/replace key and Send keys to active applications
TROJ_SUB722_P9: Gather more info
TROJ_SUB722_P10: Get cached, Screensaver, RAS, AIM, recorded e-mail passwords
TROJ_SUB722_P11: Scan for running network services
TROJ_SUB722_P12: ICQ takeover

TROJ_SUB722_SIN: This is one of the notification tools of TROJ_SUB722. It monitors online TROJ_SUB722 servers, and when servers go online with the Static IP Notification enabled and which are using UDP ports, this program receives a notification of connection. The hacker/perpetrator then gains information regarding the server's status and the compromised system's IP address. The hacker can then use the Client (detected as TROJ_SUB722) program to control/access the host computer. The client side of this Trojan has a user interface where the below information is displayed:

Title: S7 SIN
listen on port <input box>?
ip port info

The name of this program, "SIN" is an acronym for "Static IP Notifier." Upon execution, it opens the port specified in the user interface. It establishes communication via UDP. For the duration of the session, it listens to the specified port and waits for packets of data from the online server containing information regarding the IP address and status. The status of the server is color-coded, with a GREEN icon indicating that it is online. When the icon is YELLOW, the Trojan is still connecting. When the color is RED, the server is off-line and will be removed from the list after 2 minutes. The tool adds the below registry keys:

HKEY_LOCAL_MACHINE\Software\SubSeven
HKEY_LOCAL_MACHINE\Software\SubSeven\SIN

TROJ_SUB7.22.D (Aliases: BackDoor-G2.svr.ldr, SUB7.22.D, BackDoor-G2.svr.gen, Backdoor.Subseven.22): This Win32 Trojan is the server side of a hacking tool. It enables a remote hacker access to an infected computer by making itself active in memory upon boot-up or when any EXE file is executed. It is a member of the Subseven family of backdoor Trojans that compromise an infected system's network security. It gives system administrator privileges to a remote user. The Trojan is installed in memory and listens to port 643 for commands from the client side of this hacking tool.